

UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: : Group Art Unit:
Patrick, K. : To Be Assigned
Serial No.:To Be Assigned : IPLaw T81/B503
: IBM Corporation
Filed:Concurrently Herewith : PO Box 12195
: RTP, NC 27709

Title: Zero Knowledge Document Comparison Between Mutually Distrustful Parties
INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

This Information Disclosure Statement is being submitted in connection with the above-identified application for patent. Applicants submit herewith patents, publications or other information of which they are aware, which they believe may be material to the patentability of this application and in respect of which there may be a duty to disclose in accordance with 37 C.F.R. § 1.56.

While this Information Disclosure Statement may be "material" pursuant to 37 C.F.R. § 1.56, it is not intended to constitute an admission that any patent, publication or other information referred to herein is "prior art" for this invention unless specifically designated as such.

In accordance with 37 C.F.R. § 1.97(g), the filing of this Information Disclosure Statement shall not be construed to mean that a search has been made or that no other material information as defined in 37 C.F.R. § 1.56(a) exists.

The attached form, PTO-1449, provides a listing of patents, publications, or other information as required by 37 C.F.R. § 1.98(a)(1).

Respectfully submitted,

By: David R. Irvin
David R. Irvin, Agent
Reg. No. 42,682

DRI/ssc
Docket: CA920020058US1
Phone: 919-543-7810 / Fax: 919-254-4330

List of Patents and Publications for
Applicant's Information Disclosure Statement

APPLICANT: Patrick, K.

(Use several sheets if necessary)

FILING DATE: To b Assign d

GROUP: To B Assign d

Ref erence Designation

US PATENT DOCUMENTS

Examiner Initials	Document Number	Date	Name	Class/Subclass	Filing Date (If. Appro.)
	5,651,069	07/22/97	Rogaway	380/28	12/08/94
	5,790,669	08/04/98	Miller et al.	380/25	07/01/96
	6,167,521	12/26/00	Smith et al.	713/200	08/29/97

FOREIGN PATENT DOCUMENTS

Document Number	Date	Country	Class/Subclass	Translation Yes No
WO00/65426	11/2/00	WIPO	G06F 1/00	X
WO00/48358	08/17/00	WIPO	H04L 9/32	X
JP11234259	08/27/99	Japan	H04L9/08	X (Abstract)
JP11234263	08/27/99	Japan	H04L9/32	X (Abstract)

OTHER ART (Including Author, Title, Data, Pertinent Pages, etc.)

Research Disclosure "A Strong Client-Server Mutual Authentication Scheme", No. 41787
p. 129, January, 1999

Riordan, J. "Access Control for Computers" IBM Patent Application,
IBM Docket CH9-2000-0012, Filed March 14, 2001, Serial Number 09/808,341

Abe, M. "Securing 'Encryption + Proof of Knowledge' in the Random Oracle Model"
NTT Inf. Sharing Platform Labs.; Nippon Telegraph & Telephone Corp., Conference 2002,
Proceedings pp.277-289

Peyravian, M. et al. "Hash-Based Encryption System", IBM Corp. Computers & Security
Vol. 18, No. 4, pp. 345-350, 1999

Shihng, Y. et al. "Group-Oriented Authentication Mechanism with Key Exchange", Dept. of Inf.
Manage, Computer Communications, vol. 21, no. 5, pp. 485-497, May 15, 1998

Aura, T. "Strategies Against Replay Attacks", Digital Systems Laboratory, Helsinki University of
Technology, IEEE, 1997

Rangan, P. "Trust Requirements and Performance of a Fast Subtransport-Level Protocol for
Secure Communication", IEEE Transactions on Software Engineering, vol. 19, no. 2,
February, 1993.

Con't

FORM PTO-1449 (Modified)

ATTY. DOCKET NO.
CA920020058US1

SERIAL NO.
TO BE ASSIGNED

List of Patents and Publications for
Applicant's Information Disclosure Statement

APPLICANT: Patrick, K.

FILING DATE: To be Assigned
GROUP: To Be Assigned

(Use several sheets if necessary)

OTHER ART (Including Author, Title, Data, Pertinent Pages, etc.)

Maurer, U. et al. "Unconditionally Secure Key Agreement and the Intrinsic Conditional Information", IEEE Transactions on Information Theory, vol. 45, no. 2, March, 1999

Halevi, S. et al. "Public-Key Cryptography and Password Protocols", ACM Transactions on Information and System Security, vol.2, no. 3, pp.230-268, August, 1999

Park, S. et al. "Security Protocol for IEEE 802.11 Wireless Local Area Network" Mobile Networks and Application 3, pp 237-246, 1998

Examiner

Date Considered

Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.